SECTION 8

NOTICES REQUIRED TO OBTAIN APPROVAL TO USE CPNI (CONT'D)

A. Mandatory Notices Regarding Solicitation (Cont'd).

3. If written notification is provided, the notice must be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to a Customer.

4. If any portion of a notification is translated into another language, then all portions of the notification must be translated into that language.

5. The Company may state in the notification that the Customer's approval to use CPNI may enhance its ability to offer products and services tailored to the Customer's needs. The Company also may state in the notification that it may be compelled to disclose CPNI to any person upon affirmative written request by the Customer.

6. The Company may not include in the notification any statement attempting to encourage a Customer to freeze third-party access to CPNI.

7. The Company's solicitation for approval must be proximate to the notification of a Customer's CPNI rights.

SECTION 8

NOTICES REQUIRED TO OBTAIN APPROVAL TO USE CPNI (CONT'D)

B. Opt-Out Notice Requirements.

The Company must provide notification to obtain Opt-Out Approval through electronic or written methods, and not by oral communication (except for one-time use of CPNI, as discussed Section 8.D. below). The contents of any such notification must comply with the requirements of Section 8.A., above, and:

1. The Company must wait a 30-day minimum period of time after giving Customers notice and an opportunity to opt-out before assuming Customer approval to use, disclose, or permit access to CPNI. The Company may, in its discretion, provide for a longer period. The Company must notify Customers as to the applicable waiting period for a response before approval is assumed.

    a. In the case of an electronic form of notification, the waiting period begins to run from the date on which the notification was sent.

    b. In the case of notification by mail, the waiting period begins to run on the third day following the date that the notification was mailed.

2. If the Company uses the opt-out mechanism it must provide notices to its Customers every two years.

SECTION 8

NOTICES REQUIRED TO OBTAIN APPROVAL TO USE CPNI (CONT'D)

B. Opt-Out Notice Requirements (Cont'd).

3. Use of E-mail: If the Company uses e-mail to provide opt-out notices, it must comply with the following additional requirements:

a. The Company must have express, verifiable, prior approval from consumers to send notices via e-mail regarding their service in general, or CPNI in particular;

b. Customers must be able to reply directly to e-mails containing CPNI notices in order to opt-out;

c. Opt-out e-mail notices that are returned to the Company as undeliverable must be sent to the Customer in another form before the Company may consider the Customer to have received notice; and

d. The subject line of the e-mail must clearly and accurately identify the subject matter of the e-mail.

e. The Company must make available to every Customer a method to opt-out that is of no additional cost to the Customer and that is available 24 hours a day, seven days a week. The Company may satisfy this requirement through a combination of methods, so long as all Customers have the ability to opt-out at no cost and are able to effectuate that choice whenever they choose.

C. Opt-In Notice Requirements.

The contents of any Opt-In Approval notification must comply with the requirements described in Section 8.A., above.

SECTION 8

NOTICES REQUIRED TO OBTAIN APPROVAL TO USE CPNI (CONT'D)

D. Notice Requirements Specific to One-Time Use of CPNI.

1. The Company may use oral notice to obtain limited, one-time use of CPNI for inbound and outbound Customer telephone contacts for the duration of the call.

2. The contents of any such notification must comply with the requirements of Section 8.A., except that the Company may omit any of the following if not relevant to the limited use for which the Carrier seeks CPNI:

   a. The Company need not advise Customers that if they have opted-out previously, no action is needed to maintain the opt-out election.

   b. The Company need not advise Customers that it may share CPNI with its Affiliate(s) or third parties and need not name those entities, if the limited CPNI usage will not result in use by, or disclosure to, an Affiliate or third party.

   c. The Company need not disclose the means by which a Customer can deny or withdraw future access to CPNI, so long as the Company explains to Customers that the scope of the approval the Company seeks is limited to one-time use.

   d. The Company may omit disclosure of the precise steps a Customer must take in order to grant or deny access to CPNI, as long as the Company clearly communicates that the Customer can deny access to his CPNI for the call.

SECTION 9

DISCLOSURE OF CPNI WITH JOINT VENTURE PARTNERS OR INDEPENDENT CONTRACTORS

The Company must obtain opt-in consent from a Customer before disclosing the Customer's CPNI to a joint venture partners or independent contractors for the purposes of marketing Communications-Related Services to that Customer. Obtaining approval using the Opt-Out Method is not permissible.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS

A. Management Safeguards.

1. Training of Company personnel will include review of this Manual by all new employees and all existing employees who have not previously done so.

2. The Company will provide additional training on an as-needed basis.

3. Company personnel will make no decisions regarding CPNI without first consulting the individual(s) listed in Section 2 of this Manual. The Company's personnel must obtain supervisory approval regarding any proposed use of CPNI.

4. In deciding whether the contemplated use of the CPNI is proper, the individual(s) listed in Section 2 will consult this Manual, applicable FCC regulations, and, if necessary, legal counsel.

5. The person(s) listed in Section 2 will personally oversee the use of approval methods and notice requirements for compliance with all legal requirements.

6. The person(s) listed in Section 2 will also ensure that the Company complies with the opt-in requirements before sharing CPNI with any joint venture partners or independent contractors.

7. Any improper use of CPNI will result in appropriate disciplinary action in accordance with established Company disciplinary policies. Any improper use shall be treated as a serious offense, and may result in suspension or termination of employment in appropriate cases. Any Company personnel making improper use of CPNI will undergo additional training to ensure future compliance.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

A. Management Safeguards (Cont'd).

8. FCC Notification of Opt-Out Failure. The Company will provide written notice within five business days to the FCC of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

a. The notice will be in the form of a letter, and will include the Company's name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether the relevant state commission(s) has been notified and whether it has taken any action, a copy of the notice provided to Customers, and contact information.

b. The Company must submit the notice even if the Company offers other methods by which consumers may opt-out.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

A. Management Safeguards (Cont'd).

9. Annual Filing of Certificate of Compliance. On an annual basis, a corporate officer of the Company will sign and file with the Federal Communications Commission (FCC) a Compliance Certificate (Appendix 1) stating his or her personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the FCC's CPNI rules. A statement will accompany the Certificate explaining how the Company's operating procedures ensure that it is or is not in compliance with the FCC's CPNI rules, as well as an explanation of any actions taken against data brokers and a summary of all Customer complaints received in the past year concerning the unauthorized release of CPNI. Additionally, the Company must report on any information it has with respect to the processes pretexters are using to attempt to access CPNI, and what steps it is taking to protect CPNI. This annual filing will be made with the FCC's Enforcement Bureau on or before March 1 in EB Docket No. 06-36, for data pertaining to the previous calendar year.

   a. The "actions against data brokers" discussed above refers to proceedings instituted or petitions filed by the Company at either at a state or federal commission, or the court system.

   b. The "summary of all Customer complaints received" refers to number of Customer complaints the Company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category of complaint, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information.

10. The Company will review these procedures on a continuing basis to ensure compliance with all FCC regulations, and will revise these procedures as needed to reflect any subsequent revisions to the applicable rules and regulations addressing CPNI.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

B. Recordkeeping.

1. The Company will maintain records of its own sales and marketing campaigns that use CPNI in files clearly identified as such. These records include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company will maintain these records in its offices for a minimum of one year.

2. The Company will maintain records of its Affiliates' sales and marketing campaigns that use CPNI in files clearly identified as such. These records will include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company will maintain these records in its offices for a minimum of one year.

3. The Company will maintain records of all instances where it discloses or provides CPNI to third parties, or where third parties are allowed access to CPNI, in files clearly identified as such. These records will include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company maintains these records in its offices for a minimum of one year.

4. The Company's policy is to maintain records of Customer approval for use of CPNI, as well as notices required by the FCC's regulations, for a minimum of one year. The Company maintains records of Customer approval and disapproval for use of CPNI in a readily-available location that is consulted on an as-needed basis.

5. The Company will maintain separate files in which it will retain any court orders respecting CPNI.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

C. Authentication and Procedural Safeguards.

1. The Company must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI.

2. The Company must properly authenticate a Customer prior to disclosing CPNI based on Customer-initiated telephone contact, online account access, or an in-store visit.

   a. Telephone Access to CPNI. The Company will only disclose Call Detail Information over the telephone, based on Customer-initiated telephone contact, if the Customer first provides the Carrier with a password, as described in Section 10.C.3., that is not prompted by the Carrier asking for Readily Available Biographical Information, or Account Information. If the Customer does not provide a password, or does not wish to create a password, the Company may only disclose Call Detail Information by sending it to the Customer's Address of Record, or, by calling the Customer at the Telephone Number of Record (rather than using Caller ID).

   - If the Customer is able to provide Call Detail Information to the Company during a Customer-initiated call without the Company's assistance, then the Telecommunications Carrier is permitted to discuss the Call Detail Information, provided by the Customer (but not other Call Detail Information).

   - If a Customer requests non-Call Detail Information CPNI, the Company need not first obtain a password from the Customer, but must nevertheless authenticate the Customer.

   - The Company need not require Customer to setup a password, but must provide the Customer the option to do so.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

C. Authentication and Procedural Safeguards (Cont'd).

b. Online Access to CPNI. The Company must authenticate a Customer without the use of Readily Available Biographical Information, or Account Information, prior to allowing the Customer online access to CPNI related to a Telecommunications Service account. Once authenticated, the Customer may only obtain online access to CPNI related to a Telecommunications Service account through a password, as described in Section 10.C.3., that is not prompted by the Company asking for Readily Available Biographical Information, or Account Information.

- The Company may choose to block access to a Customer's account after repeated unsuccessful attempts to log into that account.

c. In-Office Access to CPNI. The Company may disclose CPNI (except for Call Detail Information) to a Customer who, in the Company's office, first presents a Valid Photo ID matching the Customer's Account Information.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

C. Authentication and Procedural Safeguards (Cont'd).

3. Establishment of a Password. The Company must authenticate the Customer without the use of Readily Available Biographical Information, or Account Information. The Company may establish passwords, among other methods:

   a. At the time of service initiation;

   b. Using a Personal Identification Number (PIN). The Company may supply the Customer with a randomly-generated PIN, not based on Readily Available Biographical Information, or Account Information, which the Customer would then provide to the Carrier prior to establishing a password. The Company may supply the PIN to the Customer by a Company-originated voicemail or text message to the Telephone Number of Record, or by sending it to an Address of Record so as to reasonably ensure that it is delivered to the intended party.

   c. The Company is not required to create new passwords for customers who already have a password, even if the password uses Readily Available Biographical Information. However, the Company must not prompt the Customer for Readily Available Biographical Information, and any back-up authentication method cannot use Readily Available Biographical Information.

4. Establishment of Back-up Authentication Methods. The Company may create a back-up Customer authentication method in the event of a lost or forgotten password. The back-up Customer authentication method may not prompt the Customer for Readily Available Biographical Information, or Account Information. The shared secret is the preferred method for establishing backup authentication.

5. Reauthentication. If a Customer cannot provide the correct password or the correct response for the back-up Customer authentication method, the Customer must establish a new password.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

6. Notification of Account Changes. The Company must notify a Customer immediately whenever a password, Customer response to a back-up means of authentication for lost or forgotten passwords, online account, or Address of Record is created or changed.

   a. This notification is not required when the Customer initiates service, including the selection of a password at service initiation.

   b. This notification may be through a Company-originated voicemail or text message to the Telephone Number of Record (not caller ID), or by mail to the Address of Record, and must not reveal the changed information or be sent to the new Account Information.

   c. A change of address should be mailed to the former address, rather than the new address.

7. Business Customer Exemption. The Company may bind itself contractually to authentication regimes other than those described in this Manual for services they provide to business Customers that have both a dedicated account representative and a contract that specifically addresses the Company's protection of CPNI.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

D. Notification of Customer Proprietary Network Information Security Breaches.

1. The Company will take reasonable steps to protect CPNI databases from hackers and other unauthorized attempts by third parties to access CPNI.

2. The Company must notify law enforcement of a Breach of its Customers' CPNI. A Breach occurs when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.

3. The Company shall not notify its Customers or disclose the Breach publicly, whether voluntarily or under state or local law or these rules, until it has completed the process of notifying law enforcement. As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the Breach, the Company shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility. The Commission will maintain a link to the reporting facility at http://www.fcc.gov/eb/cpni. The Company will indicate its desire to notify its Customer or class of Customers immediately concurrent with its notice to the USSS and FBI.

   a. Notwithstanding any state law to the contrary, the Company shall not notify Customers or disclose the Breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided in the following Paragraphs b. and c.

   b. If the Company believes that there is an extraordinarily urgent need to notify any class of affected Customers sooner than otherwise allowed under Paragraph a. immediately above, in order to avoid immediate and irreparable harm, it shall so indicate in its notification and may proceed to immediately notify its affected Customers only after consultation with the relevant investigating agency. The Company shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such Customer notification.

SECTION 10

COMPANY SAFEGUARDS AND RECORDKEEPING REQUIREMENTS (CONT'D)

D. Notification of Customer Proprietary Network Information Security Breaches (Cont'd).

c. If the relevant investigating agency determines that public disclosure or notice to Customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the Company not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the Company when it appears that public disclosure or notice to affected Customers will no longer impede or compromise a criminal investigation or national security. The agency will provide in writing its initial direction to the Company, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by Carriers.

4. After the Company has completed the process of notifying law enforcement as described in Paragraphs 3.a – 3.c. above, it shall notify Customers of the Breach.

5. Recordkeeping. The Company must maintain a record, electronically or in some other manner, of any Breaches discovered, notifications made to the USSS and the FBI pursuant to the above paragraphs, and notifications made to Customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the Breach, and the circumstances of the Breach. The Company must retain the record for a minimum of 2 years.

APPENDIX 1

ANNUAL CERTIFICATE OF COMPLIANCE WITH CPNI RULES

Including—

FILING INSTRUCTIONS AND ACCOMPANYING COVER LETTER TO THE FCC

Revised January 2010

Filing Instructions

Attached is a model Certificate of Compliance with the FCC's CPNI rules. It contains blanks for the insertion of Company-specific information. **The Certificate must be signed by an officer (e.g., the President, V.P.) of the Company.** Electronic copies of the Certificate and cover letter may be obtained from the Telecommunications Association of Michigan.

The FCC's CPNI rules state that a carrier must file a "compliance certificate" each year that addresses compliance with the FCC's CPNI regulations, along with:

- A "statement accompanying the certificate" to explain how its operating procedures ensure compliance with the FCC's CPNI regulations;
- An explanation of any actions taken against data brokers; and
- A summary of all Customer complaints received in the past year concerning the unauthorized release of CPNI.

The attached Certificate of Compliance addresses these subjects in a single document. Also attached is a sample cover letter to accompany the filing.

The FCC's CPNI rules apply to all "telecommunications carriers," which are defined to include providers of interconnected VoIP service. **You should ensure that all entities that would meet the definition of "telecommunications carrier" file a certificate.** In cases of doubt, you should consult the Telecommunications Association of Michigan or legal counsel. **The FCC has previously proposed substantial fines for carriers who inadvertently omitted their parent company, an affiliate, or a subsidiary that met the definition of "telecommunications carrier" from their Certificate.**

This Certificate of Compliance must be filed with the FCC on or by March 1 each year relating to the prior calendar year. Be sure to carefully follow the instructions below.

Simply filing the model Certificate is not enough. Your Company must make sure that it actually engages in the practices discussed in the Certificate before signing and filing it. Please read it carefully.

The procedures for filing are described on the following page. **Electronic filing is recommended unless the Certificate contains confidential information on the Company's method of combating pretexting (See Paragraph 16 of the Certificate; consultation with legal counsel is advisable).** Mailed filings are not deemed to be filed until actually received from the FCC (47 CFR 1.7). Thus, paper filings should be sent several days before they are due.

ELECTRONIC PAPERLESS FILING:

The easiest way to file is electronically through the FCC's Electronic Comment Filing System (ECFS): http://www.fcc.gov/cgb/ecfs/. Put both the completed cover letter and Certificate in a single PDF. Click on "Submit a Filing" on the left side of the screen. In completing the transmittal screen, filers should include their full name, U.S. Postal Service mailing address, and the proceeding number, which is 06-36. Under "Document Type," select "Statement."

One (1) additional copy must go to: Best Copy and Printing, Inc., 445 12th Street, Suite CY-B402, Washington, DC 20554, or via e-mail at **FCC@BCPIWEB.COM**. The draft cover letter reflects e-mail service (see the bottom of the page). Carriers who send copies via U.S. Mail should modify the cover letter accordingly.

PAPER FILING:

Companies that choose to file by paper must file an original and four (4) copies of each filing. Filings can be sent by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail.

All U.S. Postal Service first class, Express Mail and Priority Mail filings must be addressed to the Commission's Secretary, Marlene H. Dortch, Office of the Secretary, Federal Communications Commission, 445 12th Street, SW, Washington, DC 20554.

Companies can also send their filings using commercial overnight mail (other than U.S. Postal Service Mail), by sending them to Commission's Secretary, Marlene H. Dortch, Office of the Secretary, Federal Communications Commission, 9300 East Hampton Drive, Capitol Heights, MD 20743.

One (1) additional copy must go to: Best Copy and Printing, Inc., 445 12th Street, Suite CY-B402, Washington, DC 20554, or via e-mail at **FCC@BCPIWEB.COM.** The draft cover letter reflects e-mail service (see the bottom of the page). Carriers who send copies via U.S. Mail should modify the cover letter accordingly.

[Company Letterhead]

Annual 47 CFR 64.2009(e) CPNI Certification
EB Docket No. 06-36

Marlene H. Dortch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street S.W.
Suite TW-A325
Washington, D.C. 20554

Re: Annual CPNI Compliance Certificate
[Insert Company Name(s)]
Form 499 Filer ID Number(s):

Dear Secretary Dortch,

In accordance with 47 CFR 64.2009(e), please find attached the Company's Annual Compliance Certificate for the previous calendar year, 20__. The Compliance Certificate includes the Company's:

- Statement explaining how its operating procedures ensure compliance with 47 CFR, Part 64, Subpart U;
- An explanation of any actions taken against data brokers; and
- A summary of all customer complaints received in the past year concerning the unauthorized release of customer proprietary network information (CPNI).

If you have any questions regarding this filing, please direct them to the undersigned.

Sincerely,

_____
[name]
[title]

_____
[date]

Enclosure
cc via e-mail: Best Copy and Printing, Inc., **FCC@BCPIWEB.COM**

CERTIFICATE OF COMPLIANCE WITH PROTECTION OF CUSTOMER PROPRIETARY NETWORK INFORMATION RULES

Including:

Statement Explaining How Operating Procedures Ensure Regulatory Compliance

Explanation of Any Actions Against Data Brokers, and

Summary of all Customer Complaints Received

_____ signs this Certificate of Compliance in accordance with § 222 of the Telecommunications Act of 1996, as amended, 47 USC 222, and 47 CFR 64.2009, on behalf of _____ Company (Company), related to the previous calendar year, 20__.

This Certificate of Compliance addresses the requirement of 47 CFR 64.2009 that the Company provide:

- A "statement accompanying the certificate" to explain how its operating procedures ensure compliance with 47 CFR, Part 64, Subpart U;
- An explanation of any actions taken against data brokers; and
- A summary of all customer complaints received in the past year concerning the unauthorized release of customer proprietary network information (CPNI).

On Behalf Of The Company, I Certify As Follows:

1. I am the _____ of the Company, I am an officer of the Company, and I am acting as an agent of the Company. My business address is _____. The Company's Form 499 Filer ID is _____.

2. I have personal knowledge of the facts stated in this Certificate of Compliance. I am responsible for overseeing compliance with the Federal Communications Commission's (FCC) rules relating to CPNI, 47 CFR 64.2001 *et seq*.

Statement Explaining How Operating Procedures Ensure Regulatory Compliance

3. I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the FCC's regulations governing CPNI.

4. The Company ensures that it is in compliance with the FCC's CPNI regulations. The Company trains its personnel regarding when they are authorized to use CPNI, when they are not authorized to use CPNI, and how to safeguard CPNI. The Company maintains a CPNI Compliance Manual in its offices for purposes of training of new and current employees, and as a reference guide for all CPNI issues. Our CPNI

Compliance Manual is updated to account for any changes in law relating to CPNI. The CPNI Manual contains key all essential information and forms to ensure the Company's compliance with CPNI regulations.

5. The Company has established a system by which the status of a Customer's approval for use of CPNI, as defined in 47 USC 222(h)(1), can be clearly established prior to the use of CPNI. The Company relies on the involvement of its high-level management to ensure that no use of CPNI is made until a full review of applicable law has occurred.

6. Company personnel make no decisions regarding CPNI without first consulting with management.

7. The Company has an express disciplinary process in place for personnel who make unauthorized use of CPNI.

8. The Company's policy is to maintain records of its own sales and marketing campaigns that use CPNI. The Company likewise maintains records of its affiliates' sales and marketing campaigns that use CPNI. The Company also maintains records of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. These records include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company maintains these records in its offices for a minimum of one year.

9. In deciding whether the contemplated use of the CPNI is proper, management consults one or more of the following: the Company's own compliance manual, the applicable FCC regulations, and, if necessary, legal counsel. The Company's sales personnel must obtain supervisory approval regarding any proposed use of CPNI.

10. Further, management oversees the use of opt-in, opt-out, or any other approval requirements, or notice requirements (such as notification to the Customer of the right to restrict use of, disclosure of, and access to CPNI), contained in the FCC's regulations. Management also reviews all notices required by the FCC regulations for compliance therewith. Before soliciting for approval of the use of a Customer's CPNI, the Company will notify the Customer of his or her right to restrict use of, disclosure of, and access to, his or her CPNI.

11. The Company maintains records of Customer approval and disapproval for use of CPNI in a readily-available location that is consulted on an as-needed basis.

12. The Company trains its personnel for compliance with all FCC requirements for the safeguarding of CPNI, including use of passwords and authentication methods for telephone access, online access, and in-store access to CPNI, and the prevention of access to CPNI (and Call Detail Information in particular) by data brokers or "pre-texters." In-store visits require valid photo identification.

13. The Company, on an ongoing basis, reviews changes in law affecting CPNI, and updates and trains company personnel accordingly.

Explanation of Actions Against Data Brokers

14. The Company has not encountered any circumstances requiring it to take any action against a data broker during the year to which this Certificate pertains. [**Or: The Company has taken the following actions against data brokers: list case name, docket or case number, and name of data broker.**]

Summary of all Customer Complaints Received

15. The following is a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI: None. [**Or: list number of customer complaints received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category of complaint, e.g., improper access by employees, improper disclosure to individuals not authorized to receive the information, or improper access to online information by individuals not authorized to view the information.**]

16. The Company does not at this point have any specific information on the processes pretexters are using to attempt to access its Customer's CPNI. [**Or, explain specific information the company has regarding the processes pretexters are using to attempt to access CPNI, and what steps it is taking to protect CPNI. If the Company has information to provide on this topic, it should submit both redacted and un-redacted versions of this form to the FCC.**]

The company represents and warrants that this certification is consistent with 47 CFR 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Date: _____ _____

APPENDIX 2

EMPLOYEE VERIFICATION OF CPNI MANUAL REVIEW

Employee Verification

Employee Name (*Please print*):

I have reviewed the Company's Customer Proprietary Network Information (CPNI) Compliance Manual and Operating Procedures and agree to comply with the procedures set forth therein.

I am also aware that any violation of the Company's CPNI Operating Procedures is subject to the disciplinary procedure set forth in the Hiawatha Communications Inc. Employee Handbook (*Section(s) 401,401(a), 401(b); Page(s) IV-1, IV-2*).

_____
Employee Signature

_____
Date

APPENDIX 3A

SAMPLE Customer CPNI PIN and Password Setup Request Notification

Hiawatha Telephone Company
108 W Superior Street
Munising, MI 49862
(906) 387-9911

Customer Action Required

Date:

John Sample
12345 Any Street
Anytown, MI 00012
Account Number: ##########
Unique PIN: 123456

Dear Customer Name:

At HTC, the privacy and security of your account is very important to us. This is why we fully comply with the federal laws and FCC regulations that require proper authentication of our customers prior to disclosing private account information.

To better protect all of your account information and allow us to provide you the best quality customer service, the FCC now requires that you establish a password, as well as two backup security questions to use in the event you forget your password, as soon as possible in order to access your HTC account. **At your earliest convenience, please call our local office at (906) 387-9911 or stop by our local office located at 108 W Superior Street, Munising, MI to set up your password and responses to the security questions.** Our office hours are 8:00 AM – 4:30 PM Monday-Friday. In order to access your account to establish the secure password and security questions, you will need your account number and the unique PIN (Personal Identification Number) listed at the top of this letter.

Please be advised you must have a password (not just the unique PIN above) created by 12/31/07. Due to recent changes in the Federal Communications Commission's rules governing customer privacy (CPNI), HTC will be implementing its new password policy effective December 10, 2007. Failure to do so will severely diminish the amount of information we will be able to divulge to you regarding your account and will also limit the types of transactions you may complete online or over the phone. For your convenience, we have provided answers to frequently asked questions on our website, www.jamadots.com, to provide additional information on this very important and mandatory change.

Thank you in advance for completing this request as soon as possible. Your protection is our priority and we need your help to complete this very important task.

Sincerely,

HTC Management

APPENDIX 3B

SAMPLE OPT-OUT NOTICE

Date: _____

PROTECTING YOUR PRIVACY

Hiawatha Telephone Company. (HTC) protects the confidentiality of its telecommunications customers consistent with applicable law, including the FCC's regulations governing Customer Proprietary Network Information (CPNI).

What Is CPNI?

CPNI is information HTC obtains or creates in the normal course of providing local or long distance telecommunications services to you. This information includes the quantity and types of telecommunications services you currently receive, how you use them and related billing information, such as call destination, location and amount of use. CPNI is made available to HTC solely by virtue of our carrier-customer relationship. CPNI does not include your telephone number, name and address since this information is typically published in a telephone directory.

What Can HTC Do With CPNI?

HTC is permitted to use CPNI to provide the telecommunications services you purchase, including billing and collections for those services. HTC can also use or disclose CPNI, without your approval, to offer enhancements to telecommunications services of the same type that you already purchase from us. For example, if you purchase basic local telephone services, HTC does not need your approval to use your customer information to offer you enhanced services such as voicemail or caller ID services.

HTC is also permitted by federal law to use, disclose, or permit access to your individually identified customer information in certain circumstances: (1) as required by law or court order; (2) with your approval; (3) in providing or marketing the services from which the customer information is derived or services necessary to or used in such services; (4) to initiate, render, bill and collect for services; (5) for the provisioning of inside wiring, installation, maintenance and repair services; or (6) to investigate fraud or to protect against unlawful or abusive use of service and to protect other users.

Examples where disclosure of CPNI is permitted without your approval:
- When you dial 911, information about your location may be transmitted automatically to a public safety agency.
- Certain information about your long distance calls is transmitted to your long distance company for billing purposes.

• We must disclose information, as necessary, to comply with court orders or subpoenas.
• We also will share information to protect its rights or property and to protect users of its services and other carriers from
fraudulent, abusive or unlawful use of services.
• We may, where permitted by law, provide information to credit bureaus, or provide information and or sell receivables
to collection agencies to obtain payment for HTC billed products and services.

HTC may also use, disclose or permit access to your customer information for the marketing of different categories of service to which you do not subscribe. However, we must obtain your approval to do so.

Disclosure of CPNI

Protecting the confidentiality of your CPNI is your right and HTC's duty under federal law. We do not sell or disclose CPNI to anyone outside of HTC or to anyone not authorized to represent us to offer products or services, or to perform functions on our behalf, except as may be required or permitted by law or authorized by you. When HTC uses agents, contractors or other companies to perform services on our behalf, we require them to protect your CPNI consistent with applicable law. HTC does not disclose CPNI to any unaffiliated third parties for use in their own marketing.

Notice of Your Rights to Restrict CPNI

You have the right under federal law to restrict our use or disclosure of and access to your CPNI. You also have the right to grant or deny access to your CPNI. This Notice seeks your consent to permit HTC to use, disclose or permit access to your CPNI for purposes of marketing other communications-related service offerings to which you do not already subscribe. Your approval will be deemed granted unless you otherwise notify us. At no time will your decision to deny approval affect the provision of any telecommunications services from HTC. However, without your approval, our ability to provide you with information on other services will be prohibited.

Restricting Our Use of CPNI

No action by you is necessary to permit us to access and use your CPNI information to offer you communications related services that may be different from the type of services you currently receive. Your approval to use CPNI may enhance HTC's ability to offer products and services tailored to your needs. You have 35 days from the date of this Notice to advise us if you DO NOT want us to use your CPNI for this purpose before approval is assumed. Only HTC and its authorized representatives will use the CPNI. You may inform us of your decision to deny access by either calling our office, in writing or by e-mail as set forth below. There is no cost to you for your decision. After the 35 days has expired, HTC may begin using your information to offer different products to you. At any time after the 35 days, however, you can change your decision by contacting us. You have

the right to disapprove, and revoke or limit access to your CPNI at any time and at no cost. Your decision will remain effective until you change it.

How To Contact HTC

Written: HTC, Attn: Subscriber Privacy, 108 W Superior Street, Munising, MI 49862
Telephone: (906) 387-9911 or Toll Free (800) 562-9741
E-mail: htccpni@jamadots.com
Telephone and e-mail are available 24 hours a day, seven days a week to allow you to opt-out whenever you choose. If you call at a time other than our regular business hours please leave a message. We will follow-up with you for confirmation of the information the following business day.

Additional information on CPNI privacy is available from the FCC via the Internet at:
http://www.fcc.gov/cgb/complaints.html
Telephone
Voice: 1-888-CALL-FCC (1-888-225-5322)
TTY: 1-888-TELL-FCC (1-888-835-5322)
Mail:
Federal Communications Commission
Consumer & Governmental Affairs Bureau
Consumer Inquiries and Complaints Division
445 12th Street, SW
Washington, DC 20554

APPENDIX 4

SAMPLE FORM FOR DISCLOSURE OF CPNI TO THIRD PARTY ON CUSTOMER'S REQUEST

Customer Proprietary Network Information
Grant of Permission to Disclose CPNI to Third Party

Pursuant to the requirements of Section 222 of the Communications Act and the FCC's CPNI Rules (subpart U of Part 64 of the FCC Rules), Hiawatha Telephone Company is unable to provide any information regarding your account to any other party without your express written permission to do so.

Your Account Billing Name _____

Your Account Billing Address _____

Your Billing Telephone Number(s) _____

I give my written permission to allow _____,
whose address is _____,
whose phone number is_____,

to receive written, and/or electronic responses for the following information on the above stated account (describe):

Signature:_____

Printed Name_____

Date:_____

You may revoke this Grant of Permission by writing to us at:

or calling us at:

For Company Use:

Customer did one of the following:

☐ Requested Call Detail Information, presented a Valid Photo ID, and established a password.
☐ Requested Call Detail Information, and provided password.
☐ Requested CPNI other than Call Detail Information, and provided password.
☐ Requested CPNI other than Call Detail Information, and presented a Valid Photo ID.
☐ Requested CPNI other than Call Detail Information, and was authenticated by a Company representative calling the Customer's Telephone Number of Record.

APPENDIX 5

Log of Customer Complaints Related to CPNI

LOG OF CUSTOMER COMPLAINTS RELATED TO CPNI

Affected Customer Name	Date of Compliant	Description of Complaint

Red Flag Rules Manual

Red Flags and Address Discrepancies

Compliance Manual and Operating Procedures

For

Hiawatha Telephone Company
Chippewa County Telephone Company
Ontonagon County Telephone Company
Midway Telephone Company

October 2008

TABLE OF CONTENTS

SECTION 1

DEFINITIONS

Account: A continuing relationship established by a person with a Creditor (like the Company) to obtain a product or service for personal, family, household or business purposes, and includes the provision of services on a deferred payment basis.

Annual Report: See Section 9.

Board of Directors: The Company's board of directors, or if the Company does not have a board of directors, a designated employee at the level of senior management.

Covered Account: An Account that the Company offers or maintains primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions. Telecommunication service accounts can be Covered Accounts. The term also includes any other Account for which there is a reasonably foreseeable risk to Customers or to the Company of Identity Theft, including financial, operational, compliance, reputation, or litigation risks (See Section 4).

Company: Hiawatha Company's

SECTION 1

DEFINITIONS (CONT'D)

Consumer Report: A written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes, employment purposes, or any other purpose authorized under 47 USC 1681 *et seq.*

Credit: The right granted by a Creditor, like the Company, to defer payment of debt or to incur debts and defer its payment or to purchase property or services on a deferred payment basis.

Creditor: A person, like the Company, who regularly extends, renews, or continues Credit, or who regularly arranges for the extension, renewal, or continuation of Credit, or any assignee of an original Creditor who participates in the decision to extend, renew, or continue Credit. Telecommunication service providers can be Creditors.

Customer: A person that has a Covered Account with a Creditor or a financial institution.

Identity Theft: A fraud committed or attempted using the Identifying Information of another person without authority.

SECTION 1

DEFINITIONS (CONT'D)

Identifying Information: A name or number that may be used, alone or in conjunction with any other information, to identify a specific person. The following are examples of Identifying Information:

- Name, Birth Date, Social Security Number, Drivers License or Identification, Alien Registration, Passport Number, Employer or Tax Identification Number;
- Unique Biometric Data, such as a Fingerprint, Voiceprint, Retina or Iris Image, or other Physical Representation;
- Unique Electronic Identification, Address, Routing Code.

Notice of Address Discrepancy: A notice from a consumer reporting agency informing the Company of a substantial difference between the address that the consumer provided and the address in the agency's file for the consumer.

Red Flag: See Section 3.

Readily Available Biographical Information: Information drawn from the Customer's life history and includes such things as the Customer's social security number (or the last four digits), mother's maiden name, home address, or date of birth.

Service Provider: A provider of a service directly to a financial institution or Creditor.

SECTION 2

STATEMENT OF CORPORATE POLICY

The policy of Hiawatha Company's is to comply with the letter and spirit of all laws of the United States, including those pertaining to Identity Theft contained in the Fair Credit Reporting Act, as amended, 15 USC 1681 *et seq.*, and the Federal Trade Commission's (FTC's) regulations, 16 CFR Part 681. The Company's policy is to protect against the risk of Identity Theft.

The FTC's regulations require the Company to establish a written Identity Theft Prevention Program, and to train its personnel accordingly. This Manual, in conjunction with the Company's Customer Proprietary Network Information (CPNI) Manual, constitutes the Company's written Identity Theft Prevention Program.

All personnel are required to follow the policies and procedures specified in this Manual.

- Any questions regarding compliance with applicable law and this Manual should be referred to Jay Brogan, President and C.E.O.

- The following individuals are responsible for oversight of the Company's Identity Theft Prevention Program:

  Jay Brogan, President and C.E.O.

- The Company's Board of Directors Approved this Manual on April 9, 2009.

SECTION 3

WHAT IS A RED FLAG?

A Red Flag is a pattern, practice or specific activity that indicates the possible existence of Identity Theft.

Examples of Red Flags:

- Alerts, notifications, or warnings from consumer reporting agencies, law enforcement, Customers, or victims of Identity Theft.
- Presentation of suspicious documents.
- Unusual use or suspicious activity related to a Covered Account.
- Presentation of suspicious personal identification information.

The purpose of this Manual is to set forth the Company's policies and procedures regarding Red Flags and the prevention and mitigation of Identity Theft.

SECTION 4

IDENTIFICATION OF COVERED ACCOUNTS

The Red Flag rules require the Company to periodically determine whether it offers or maintains Covered Accounts.

The Company will treat all Accounts involving the provision of service on a deferred-payment basis to the public (including residential and business services), as Covered Accounts.

The Company will, on an ongoing basis, determine whether any Accounts that it has not previously treated as Covered Accounts, should be treated as Covered Accounts, taking into consideration:

- The methods of opening Accounts;
- The methods of access to Accounts; and
- Previous experiences with Identity Theft.

SECTION 5

OVERVIEW OF IDENTITY THEFT PREVENTION PROGRAM

The Company endeavors to detect, prevent and mitigate Identity Theft (1) in connection with the opening of a Covered Account, and (2) with respect to existing Covered Accounts.

The Company will—

1. Identify relevant Red Flags for the Covered Accounts that the Company offers or maintains (see Section 6);

2. Detect Red Flags (see Section 6);

3. Take appropriate action to prevent and mitigate any detected Red Flags (see Section 7); and

4. Periodically update this Manual to reflect changes in risks to Customers and to the safety and soundness of the Company from Identity Theft (see Section 8).

SECTION 6

IDENTIFYING RED FLAGS

OPENING OF NEW ACCOUNTS

The Company has determined that a reasonably foreseeable risk of Identity Theft exists when prospective Customers seek to open new Accounts. The Company will therefore use reasonable measures to identify a person or entity that seeks to open a Covered Account.

This Section 6 therefore identifies Red Flags applicable to the opening of new Covered Accounts, and establishes the Company's method of detecting such Red Flags.

The Company will not open a Covered Account or provide any service until it is able to satisfactorily identify the prospective Customer in accordance with this Section 6. If the Company detects a Red Flag during the process of opening a Covered Account, it will place the opening of the Covered Account on hold until it can satisfactorily resolve the Red Flag.

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

OPENING OF NEW ACCOUNTS (CONT'D)

A. Opening of Covered Accounts for Personal, Family or Household Purposes.

1. Required Information: When a prospective Customer seeks to open a Covered Account for residential service (i.e., for personal, family or household purposes), the Company will ask for the following from the prospective Customer:

   - name;
   - address;
   - birth date;
   - an unexpired government-issued identification bearing a photograph, such as a driver's license or passport.

   The Company will also encourage (but not require) Customers to establish passwords as a means of protecting against potential future Identity Theft.

   The Company will encourage Customers who establish passwords not to use Readily Identifiable Biographical Information.

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

OPENING OF NEW ACCOUNTS (CONT'D)

A. Opening of Accounts for Personal, Family or Household Purposes (Cont'd).

2. Identification Confirmation.

a. The Company will make a photocopy of the prospective Customer's identification, and will inspect the identification for any signs of falsification, such as:

- misspellings;
- a photo that does not resemble the prospective Customer;
- inconsistencies in color, texture or images (such as erasures or smudges);
- raised edges around a photograph indicating the placement of a second photograph over an original photograph;
- card wear inconsistent with date of issuance (such as an identification that appears new but bears an issuance date of many years);

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

OPENING OF NEW ACCOUNTS (CONT'D)

A. Opening of Accounts for Personal, Family or Household Purposes (Cont'd).

2. Identification Confirmation (Cont'd).

b. Address Discrepancies.

If a prospective Customer provides an address to the Company that does not match the prospective Customer's identification, the Company will verify the validity of the prospective Customer's address. The following are examples of methods that the Company may utilize:

- If the prospective Customer recently moved to the area, the Company will request proof of the recent move. Examples include: moving company's receipt, sticker on valid driver's license, voter registration card, utility bill, piece of mail with forwarding sticker.

- The Company may choose to order a Consumer Report with respect to the prospective Consumer as a tool to confirm identity. Before ordering a Consumer Report, the Company will obtain the prospective Customer's written approval (see Appendix 3). The Company may quiz the prospective Customer regarding non-public information contained therein. The Company may also choose to employ the services of a third-party Identity Theft detection agent.

c. The Company will create a record of the means used to verify a Customer's identity. The Company will retain such record until 5 years after the Account is closed. Upon disposal, the Company will completely destroy the record.

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

OPENING OF NEW ACCOUNTS (CONT'D)

B. Opening of Business Accounts.

For a prospective business Customer, the Company will require documents to verify the existence of the business. Such documents may include:

- Articles of Incorporation or Articles of Limited Liability Company and evidence of filing of same with the Michigan Department of Labor and Economic Growth.
- Partnership agreement.
- Trust instrument.
- Federal Tax ID document

A sole proprietorship may use an "assumed name" document filed with the Department of Labor and Economic Growth, or the personal information of the sole proprietor.

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

OPENING OF NEW ACCOUNTS (CONT'D)

C. Examples of Red Flags in the Opening of New Accounts.

1. Suspicious Documents and Personal Identifying Information.

a. Information on the identification is inconsistent with information provided by the person opening a new Covered Account.

b. Information on the identification is inconsistent with readily accessible information, such as a signature on a check.

c. Documentation that appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

d. An address not matching any address in a Consumer Report;

e. Documents provided for identification appear to have been altered or forged (discussed above).

SECTION 6

IDENTIFYING RED FLAGS (CONT'D)

OPENING OF NEW ACCOUNTS (CONT'D)

C. Examples of Red Flags in the Opening of New Accounts (Cont'd).

2. Unusual Use of, or Suspicious Activity Related to, the Covered Account.

a. A Covered Account is used in a manner inconsistent with established patterns of activity, such as a material change in telephone local and toll calling patterns;

b. Usage of a Covered Account that has been inactive for a reasonably lengthy period of time.

c. A Customer advises that the Customer is not receiving monthly bills from the Company.

d. A Customer advises of unauthorized charges or transactions in connection with a Covered Account.

3. The Company receives notice from a Customer, a victim of Identity Theft, law enforcement, or any other person that it may have opened an Account for a person engaged in Identity Theft.